AMENDMENTS TO THE SPECIFICATION

PLEASE AMEND paragraph **0012** by replacing it with the following:

[0012] Another need addressed by the inventions is dispensing with the need for the modulus in the multiplicative group xy modulo p to be fixed ~~with respect~~ with respect to the order of the input and output set. The IDEA cipher uses a multiplicative group modulo $p = 2^{16} + 1$ (which is prime) along with two other group operations to encrypt binary data in the set of 16-bit integers, but very few known moduli have the desirable property of being exactly one greater than a power of two. The result is an undesirable lack of scalability.

PLEASE AMEND paragraph **0028** by replacing it with the following:

[0028] FIG. 6 illustrates the document of FIG. 5 with a simulated digital signature that resides in a graphic within a signature block that is excluded from the signature calculation of the document.

PLEASE AMEND paragraph **0084** by replacing it with the following:

[0084] Bob needs no further convincing that Alice was the one who signed the purchase agreement. His lawyer, however, wants him to check out SelfCertify.com's SSL certificate for the copied ACI. Bob downloads the ACI copy from SelfCertify.com and, with the image of the ACI in his Web browser, clicks on the "security" button of the browser. The browser provides a certificate issued to SelfCertify.com from a major CA, and Bob's lawyer is satisfied.

PLEASE AMEND paragraph **0131** by replacing it with the following:

[0131] The document's signature can be verified simply by opening it with a customized TIFF reader, which will detect the presence of the signature region and will validate the signature within it against the data of the document except the graphics within the

signature block. An option can be provided to put the signature data on ~~and~~ an entirely separate page of the document (*e.g.*, after the last page), preferably with a facsimile copy of the signer's ACI. (In such embodiments, the ACI should have a blank space for the signature data of the document signed with the ACI's signing key.)

PLEASE AMEND paragraph **0132** by replacing it with the following:

[0132] An exemplary process 400 is illustrated in FIG. 4, in which a signer creates a document 410 (e.g., a letter) using whatever software he (or she) wishes to use (e.g., MICROSOFT WORD 97). At 412, the signer prints the document to the SelfCertify.com virtual TIFF printer, which acts [as] as a "software signature machine." The printer driver software creates a TIFF file of the document and displays it in a viewer window. The user interface of the viewer window requests that the signer select a graphical region within the displayed document for application of the signer's digital signature "stamp."

PLEASE AMEND paragraph **0133** by replacing it with the following:

[0133] The user can specify the region by moving a dashed box around the screen, as illustrated in FIG. 5. Dashed box 510 appears over text of a document to be signed 500. Dashed box 510 includes left and right arrows 512, 514 within it for navigating to different pages of a multi-page document, and ~~a[n]~~ a "sign here" (or "OK") button 516 for applying the digital signature "stamp" at the current location of the box. FIG. 5 shows what box 516 might look like as it is moved around during the selection process.

PLEASE AMEND paragraph **0161** by replacing it with the following:

[0161] The (A,B) output of block 1530 is applied to a secure encryption and delay block 1550. Using an inventive indexed key lookup, block 1550 operates with a number of cycles selected to give about a ~~third-sec[.]ond~~ third-second delay on the user's machine. A third-second delay multiplied by eight (the number of times block 1550 iterates, the

number of consonant-vowel pairs accepted by user interface 1510) totals about 2.5 seconds and is not very noticeable.

PLEASE AMEND paragraph **0189** by replacing it with the following:

[0189] When performing a pseudogroup operation with p < M, key values should be less than p. ~~TABLE V below shows an example[s] of such an operation, with an~~ TABLE V below shows an example of such an operation, with an unrealistically small but illustrative value of p.